

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

LINDABETH RIVERA, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Civil Action No. 1:16-cv-02714

Judge: Hon. Edmond E. Chang

Magistrate Judge: Hon. Michael T. Mason

JOSEPH WEISS, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Civil Action No. 1:16-cv-02870

Judge: Hon. Edmond E. Chang

Magistrate Judge: Hon. Michael T. Mason

**PUBLICLY FILED
REDACTED VERSION**

**PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION FOR
SUMMARY JUDGMENT ON STANDING AND RELATED DEFENSES**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	FACTUAL AND PROCEDURAL BACKGROUND	3
	A. Statement of Facts	3
	B. Procedural Background	4
III.	APPLICABLE LEGAL STANDARD	5
IV.	ARGUMENT	6
	A. Plaintiffs Have Standing.....	6
	1. BIPA Statutorily Recognizes a Reasonable Expectation of Privacy Closely Related to the Deepest Roots of the Right of Privacy.....	8
	2. Applicable Precedent Supports Plaintiffs’ Standing.....	11
	3. The Violation Plainly Caused the Injury.....	15
	B. Plaintiffs Are Aggrieved Within the Meaning of BIPA.....	16
	1. Plaintiffs Are Aggrieved As a Matter of Statutory Interpretation.....	16
	2. Plaintiffs Are Aggrieved As a Matter of Precedent.....	17
	C. Plaintiffs Are Entitled to Statutory Damages and Injunctive Relief.....	20
	1. Statutory Damages.....	20
	2. Injunctive Relief.....	22
V.	CONCLUSION.....	24

TABLE OF AUTHORITIES

CASES

<i>Adickes v. S.H. Kress & Co.</i> , 398 U.S. 144, 157 (1970).....	5
<i>Allstate Ins. Co. v. Menards Inc.</i> , 285 F.3d 630, 635 (7th Cir. 2002).....	18
<i>American Surety Co. v. Jones</i> 51 N.E.2d 122 (Ill. 1943).....	17, 18, 19
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242, 248 (1986).....	5
<i>Braitberg v. Charter Communications, Inc.</i> , 836 F.3d 925 (8th Cir. 2016).....	12
<i>Celotex Corp. v. Catrett</i> , 477 U.S. 317, 322 (1986).....	5
<i>Doe v. Chao</i> 540 U.S. 614 (2004).....	20, 21, 22
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979, 983 (9th Cir. 2017).....	12
<i>Glos v. People</i> 102 N.E. 763, 766 (Ill. 1913).....	17
<i>Groshek v. Time Warner Cable, Inc.</i> , 865 F.3d 884 (7th Cir. 2017).....	12
<i>Gubala v. Time Warner Cable, Inc.</i> , 846 F.3d 909 (7th Cir. 2017).....	12
<i>Hancock v. Urban Outfitters, Inc.</i> , 830 F.3d 511 (D.C. Cir. 2016).....	12
<i>In re Facebook Biometric Information Privacy Litig.</i> , No. 3:15-cv-03747-JD, 2018 WL 1794295, at *7 (N.D. Cal. Apr. 16, 2018).....	17, 21
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , No. 16-MD-02752-LHK, 2018 WL 1243332, *1-3 (N.D. Cal. Mar. 9, 2018).....	1

<i>Jaskowski v. Rodman & Renshaw, Inc.</i> , 842 F. Supp. 1094, 1096 (N.D. Ill. 1994)	6
<i>Kehoe v. Fidelity Federal Bank & Trust</i> 421 F.3d 1209 (11th Cir. 2005).....	22
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555, 560 (1992).....	6
<i>McCullough v. Smarte Carte, Inc.</i> , No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).....	14
<i>Monroy v Shutterfly</i> , 2017 WL 4099846 (U.S. Dist. Ct. N.D. Ill December 21, 2017).....	14
<i>Padilla v. DISH Network L.L.C.</i> , No. 12-cv-7350, 2014 WL 539746 (N.D. Ill. Feb. 11, 2014).....	21
<i>Patel v. Facebook, Inc.</i> , 290 F. Supp. 3d 948.....	11
<i>Pichler v. UNITE</i> 542 F.3d 380 (3d Cir. 2008).....	22
<i>Pub. Citizen v. Dept. of Justice</i> , 491 U.S. 440 (1989).....	7
<i>Robins v. Spokeo, Inc.</i> , 867 F.3d 1108, 1117 (9th Cir. 2017).....	7
<i>Rosenbach v. Six Flags Entertainment Corp.</i> , 2017 Ill. App. 2d 170317 (Ill. App. Ct. 2017).....	18
<i>Sierra Club v. Franklin County Power of Ill.</i> , 546 F.3d 918, 935 (7th Cir. 2008).....	23
<i>Spokeo, Inc. v. Robins</i> , 136 S. Ct. 1540, 1547 (2016).....	6
<i>Sterk v. Redbox Automated Retail, LLC</i> , 672 F.3d 535 (7th Cir. 2012).....	21
<i>Trannel v. Prairie Ridge Media, Inc.</i> , 987 N.E.2d 923 ¶¶ 14-15 (Ill. Ct. App. 2013).....	9
<i>Van Alstyne v. Electronic Scriptorium, Ltd.</i> , 560 F.3d 199 (4th Cir. 2009).....	21

<i>Vigil v. Take-Two Interactive Software, Inc.</i> , 235 F. Supp. 3d 499 (S.D.N.Y. 2017).....	13
---	----

<i>Weber-Stephen Prods. LLC v. Sears Holding Corp.</i> , 145 F. Supp. 3d 793, 798 (N.D. Ill. 2015).....	5, 6
--	------

STATUTES

740 Ill. Comp. Stat. Ann. §§ 14/1-14/30 (“BIPA”).....	1
740 Ill. Comp. Stat. Ann. §§ 14/15(c).....	1
740 Ill. Comp. Stat. Ann. §§ 14/10.....	1,9
740 Ill. Comp. Stat. Ann. §§ 14/15(b)	2
740 Ill. Comp. Stat. Ann. §§ 14/15(d)	2
740 Ill. Comp. Stat. Ann. §§ 14/15(a)	2
Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681.....	7
765 Ill. Comp. Stat. Ann. § 1075/213.....	10
740 Ill. Comp. Stat. Ann. § 14/10.....	13
740 Ill. Comp. Stat. Ann. § 14/20.....	16, 20, 21

OTHER AUTHORITIES

The New Wigmore: Evidentiary Privileges § 5.3.3, at 475-76 (3d ed. 2017).....	8
Restatement (Second) of Torts § 652A (1977).....	8
Restatement (Second) of Torts § 652B (1977)	10
Restatement (Second) of Torts § 652C (1977)	10

Plaintiffs Lindabeth Rivera (“Ms. Rivera”) and Joseph Weiss (“Mr. Weiss”) (collectively, “Plaintiffs”) submit this response in opposition to the Motion for Summary Judgment on Standing and Related Defenses (the “Motion”) filed by defendant Google LLC (“Google”).¹

I. INTRODUCTION

Through this Motion Google, the world’s biggest information trafficker, seeks *carte blanche* to gather biologically-determined, immutable identifying information on anyone and everyone. The Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. §§ 14/1-14/30 (“BIPA”), clearly prohibits such intrusive behavior. As a civil statute, the sole enforcement mechanism under BIPA is a private right of action rather than criminal prosecution, but Google asks the Court to nullify that private right of action and, thus, to emasculate the entire statute. The Court should deny that request, and should deny Google’s Motion.

Biometrics are unique, physiologically-dictated characteristics that, unlike social security numbers, driver’s license numbers, or credit-card numbers, are part of our personal identities as human beings. *Id.* § 14/15(c). As BIPA explicitly states, identifiers such as “scan[s] of hand or face geometry” are especially sensitive because they cannot be changed in the event of theft or other security breach. *Id.* §§ 14/5(c), 14/10. And while Google assures us that it is storing such information securely, it simply is not possible to predict whether Google will be able to prevent data breaches such as those that have affected competitors like Yahoo in the long run.²

For good reason, the State of Illinois therefore put its citizens in the driver’s seat, requiring fully informed, written consent before anyone may “collect, capture, purchase, receive through

¹ For the sake of simplicity, citations to the record are to case number 1:16-cv-02714 filed by plaintiff Rivera, except where a difference between the records in the two cases warrants otherwise.

² See, e.g., *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2018 WL 1243332, *1-3 (N.D. Cal. Mar. 9, 2018) (describing multiple Yahoo data breaches).

trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information.” *Id.* §14/15(b). Separate provisions further prohibit disseminating, trading in, or profiting from those biometrics, *id.* § 14/15(c), (d), and regulate retention and destruction of such information, *id.* § 14/15(a), (e).

The behavior at issue in this case is far different from the routine and transparent collection of names, addresses, social security numbers, and credit card numbers that occurs during and in aid of consumer transactions. Biometric identifiers are based on biological traits and, rather than being designed by humans to facilitate economic transactions, represent part of who we are as humans. Violation of BIPA requires complicated volitional actions using sophisticated technological means, subject in this case to patents owned by Google. Absent carefully informed consent, the acquisition and retention of such information is aberrant, intrusive, and offensive. The State of Illinois was well within its plenary constitutional authority to prohibit, or even criminalize, what Google is doing.

Plaintiffs need not prove pecuniary or other property loss to have standing or to be aggrieved. The State of Illinois acted squarely within the historical path of American privacy law by recognizing its citizens' right to control the creation, use, maintenance, and destruction of their own biologically determined identifiers and information. Google trampled on those rights and asks to continue. It mapped Plaintiffs' faces, creating, collecting, storing, and exploiting their unique biometric identifiers for its own competitive advantage in the marketplace for photo-sharing services. Unlike the aforementioned social security or credit card numbers, Plaintiffs' biometric identifiers should not even be in Google's possession, and would not be but for Google's lawless behavior. It makes no difference that Plaintiffs did not shun photography after learning of Google's intrusion, because it was too late to matter — Google already illegally had arrogated

their biometrics. The remedy lies not in the futile act of ducking the camera, but in the power of this Court to stop Google's flagrant violation of Illinois law.

The Motion should be denied.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Statement of Facts

This Court previously summarized the salient facts alleged in the Complaint:

Between around March 2015 and March 2016, "approximately eleven" photographs of Lindabeth Rivera were taken in Illinois by a Google Photos user on a Google Droid device. The person who took the picture was an Illinois resident who had purchased the Droid device in Illinois. As soon as the photographs of Rivera were taken, the Droid automatically uploaded them to the cloud-based Google Photos service. According to the Complaint, Google immediately scanned each uploaded photograph of Rivera. The scans located her face and zeroed in on its unique contours to create a "template" that maps and records her distinct facial measurements. At the time of the automatic upload and face-scan, the photographer's Droid device was still in Illinois and would have had an Illinois-based Internet Protocol (IP) address.

Weiss's experience was similar, except that Weiss himself was a user of Google Droid and Google Photos (Rivera, on the other hand, neither had a Droid nor a Google Photos account). Between 2013 and 2016, Weiss took "approximately twenty-one" photos of himself while in Illinois on his Droid device. These photos were automatically uploaded when they were taken, and then immediately scanned to create a custom face-template based on Weiss's features. At the time of uploading and scanning, Weiss's Droid was in Illinois and it would have had an Illinois-based Internet Protocol (IP) address.

Both Rivera and Weiss contend that their face templates were then used by Google to find and group together other photos of them. Google also used the templates to recognize their gender, age, race, and location. At no time was Rivera's or Weiss's consent sought by Google to create or use the face-templates. Nor did Rivera or Weiss give Google permission to collect or store the data derived from their faces.

(ECF No. 60 at 2-4 (citations omitted).)

The evidence developed in discovery has fully borne out the allegations of the Complaint. The evidence demonstrates, and Google does not actually dispute, that Google captured, stored,

and used face scans of Plaintiffs. (*See* Plaintiff’s Statement of Additional Facts (“SAF”) 1.) Furthermore, despite Google’s protestations that Plaintiffs’ conduct somehow immunizes it from liability for its violation of Illinois law, Google does not and cannot dispute that it lacked permission from Plaintiffs to capture, store, and use those face scans. (SAF 2.)

As Plaintiff Weiss testified at his deposition: “I believe that my biometric information or identifier is very sensitive. I think it’s akin to my DNA, to a fingerprint. To have that stored, collected, is, again, that in and of itself, when done so against my consent or without my consent, it’s a damage, I think.” (SAF 3 (quoting Maya Decl. Ex. A (Weiss Depo) at 176:21-177:2).) Plaintiff Rivera proffered similar testimony demonstrating her real and concrete injuries from Google’s unauthorized collection, use, and storage of her biometrics. (SAF 4.) For instance, she “feel[s] like Google taking [her biometric information] without consent” makes it “easier for other outside people to get access to something that’s very unique to me that I can’t necessarily change.” (*Id.* (quoting Maya Decl. Ex. B (Rivera Depo) at 78:10-14).)

And while Google makes much of its self-serving statements that this sensitive data, taken without permission in violation of Illinois law, is being held securely, it is beyond dispute that the biometric information is accessible to Google, its personnel, and to any party that Google permits (willingly or otherwise) to access the data. (*See* Plaintiffs’ Response to Google’s Statement of Undisputed Fact (“Response to SUF”) 20; Porter Decl. ¶¶ 4-10.) Google has patented the technologies at issue, and profits from them. (SAF 5-6.) Google Photos is automatically loaded on many phones running the Android operating system, and it appears that Google creates face templates (*i.e.*, collects biometric information) from every face uploaded to its cloud service whether or not users click or un-click any particular setting. (*See* Response to SUF 10; SAF 7.)

B. Procedural Background

The Motion is Google's third attempt to derail these proceedings. On May 18, 2016, Google filed a motion to dismiss based on several theories: that BIPA does not apply to photographs and information derived from photographs, that BIPA has impermissible extraterritorial effects, and that BIPA violates the Dormant Commerce Clause of the U.S. Constitution. (ECF No. 34.) Applying a "straightforward reading" of the statute on February 27, 2017 (ECF No. 60 at 11), this Court rejected Google's arguments as unsupported by the statutory text (*id.* at 11-17) and contrary to the legislative history set forth in the statute itself (*id.* at 17-21).

On March 9, 2017, unsatisfied with the Court's decision, Google moved for permission to seek interlocutory review and for a stay pending such review. (ECF No. 67.) On June 27, 2017, the Court denied that motion as well. (ECF No. 76.)

The parties filed a joint status report on March 28, 2018, proposing a briefing schedule for the present motion for summary judgment (ECF No. 137). The Court approved the proposed schedule (ECF No. 141), and Google filed the Motion on April 23, 2018 (ECF No. 154).

III. APPLICABLE LEGAL STANDARD

Summary judgment is appropriate only if "the pleadings, depositions, answers to interrogatories and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c). "A genuine dispute exists if 'the evidence is such that a reasonable jury could return a verdict for the nonmoving party.'" *Weber-Stephen Prods. LLC v. Sears Holding Corp.*, 145 F. Supp. 3d 793, 798 (N.D. Ill. 2015) (Chang, J.) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). The moving party bears the heavy burden of demonstrating the absence of *even one* genuine issue of material fact. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 157 (1970).

A fact is material if it could affect the outcome of the suit under the governing law. *Anderson*, 477 U.S. at 248-49. And Google has laid out what it contends are material facts in its Statement of Undisputed Fact (“SUF”). (Docket No. 153.) Plaintiffs demonstrate that many of Google’s statement of fact are disputed and present triable issues in their concurrently filed Response to that SUF.

A court “must view the facts and draw reasonable inferences in the light most favorable to the non-moving party” and “must not weigh conflicting evidence or make credibility determinations.” *Weber-Stephen*, 145 F. Supp. 3d at 798. A court should act “with caution” in determining summary judgment. *Anderson*, 477 U.S. at 255. Accordingly, “[s]ummary judgment should be denied ‘where there is reason to believe that the better course would be to proceed to a full trial.’” *Jaskowski v. Rodman & Renshaw, Inc.*, 842 F. Supp. 1094, 1096 (N.D. Ill. 1994) (quoting *Anderson*, 477 U.S. at 255).

IV. ARGUMENT

Plaintiffs have standing, are aggrieved within the meaning of BIPA, and are entitled to statutory damages and injunctive relief.

A. Plaintiffs Have Standing

Standing is a judicially created doctrine intended to keep judicial power within the constitutionally prescribed arena of cases and controversies. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). To have standing, a plaintiff must have “(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Id.* The Motion argues that Plaintiffs have not suffered an injury in fact.

The injury-in-fact requirement means that a plaintiff must have “suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* at 1548 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555,

560 (1992)). “A ‘concrete’ injury must be ‘*de facto*’; that is, it must actually exist.” *Id.* “‘Concrete’ is not, however, synonymous with ‘tangible.’” *Id.* at 1549. “[I]ntangible injuries can nevertheless be concrete.” *Id.* After all, “the law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure,” *id.*, as with libel and slander, *id.*, or, one might add, as with other non-pecuniary harms like pain and suffering, or emotional distress. Thwarting an intangible, non-pecuniary statutory right can likewise work a concrete injury, as in the deprivation of a right to government information. *See id.* at 1549-50 (citing *FEC v. Akins*, 524 U.S. 11 (1998); *Pub. Citizen v. Dept. of Justice*, 491 U.S. 440 (1989)). Even a “risk of real harm” can satisfy the requirement of concreteness. *Id.* at 1549.

Legislation is entitled to no less respect than common-law judicial decision-making in recognizing legal rights. Accordingly, in determining whether intangible harms qualify as sufficiently concrete, “both history and the judgment of Congress play important roles.” *Id.* A court should consider “whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts,” and should consider the judgment of Congress (or in the present case, the Illinois Legislature) in identifying intangible harms and elevating them to the status of legally cognizable injuries. *Id.*

The plaintiff in *Spokeo*, for example, brought a claim under the Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681i, against the operator of a “people search” website on which plaintiff’s education, family status, and economic status were misrepresented. *Spokeo*, 136 S. Ct. at 1544; *id.* at 1556 (Ginsburg, J., dissenting). The Supreme Court offered the illustration that misrepresenting the plaintiff’s zip code could not work any concrete harm, *id.* at 1550, but left to the Ninth Circuit on remand the question whether the other misrepresentations could be concrete, *id.* n.8. On remand, the Ninth Circuit held that the plaintiff had standing because

misrepresentations about his education, family, and economic status posed a real risk of harm sufficient to satisfy the concreteness requirement. *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1117 (9th Cir. 2017) (“Robins’s allegations relate facts that are substantially more likely to harm his concrete interests than the Supreme Court’s example of an incorrect zip code.”).

Applied to the present case, these principles confirm that Plaintiffs have standing.

1. BIPA Statutorily Recognizes a Reasonable Expectation of Privacy Closely Related to the Deepest Roots of the Right of Privacy

The right to privacy is a particularly American legal concept, but at this point is well established and deeply rooted. Its origins are widely acknowledged to trace back to a seminal article in the Harvard Law Review. *See* Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). The development of the right to privacy was fueled by social and technological change. Urbanization compromised privacy and “[t]echnological developments intensified the threat.” 1 Edward J. Irmwinkler, *The New Wigmore: Evidentiary Privileges* § 5.3.3, at 475-76 (3d ed. 2017) (footnote omitted). “[B]reakthroughs in aural and visual surveillance devices seemed to outflank personal privacy,” *id.* at 476 (alteration, internal quotation marks and footnote omitted), and “[s]uch books as Vance Packard’s *The Naked Society* and George Orwell’s *Nineteen Eighty-Four* struck a responsive chord . . . because the public had become alarmed about the magnitude of the threat to privacy,” *id.* (footnotes omitted).

By the mid-twentieth century, hundreds of appellate opinions had recognized a right of privacy in one context or another. *See id.* at 479. Dean and tort-law scholar William Prosser synthesized the cases into four categories: “appropriation, unreasonable intrusion, public disclosure of private facts, and false light in the public eye,” *id.*, and “[a]s a generalization, that thesis holds true even today,” *id.* at 480. The Restatement section cited in the Motion follows that formulation. *See* Restatement (Second) of Torts § 652A (1977).

BIPA is a direct descendant in this legal lineage. The development and large-scale feasibility of powerful new biometric identification technologies addressed by BIPA — retina scans, iris scans, voiceprints, and scans of hand or face geometry, *see* 740 Ill. Comp. Stat. Ann. § 14/10 — has commenced the latest chapter in the long history of the American right to privacy.

In a sense, biometric identifiers are nothing new, as the inclusion of fingerprints in BIPA’s coverage attests. But never before have powerful entities like the defendant in this case so brazenly usurped the public’s expectation of privacy by collecting such information. If fast-food restaurants had conducted a campaign to dust customers’ trays for fingerprints and store those prints in a massive database, perhaps BIPA or something like it would have been enacted sooner. But Big Brother had not yet arrived.

BIPA is not only in line with the history of privacy; it is at home within the seminal thesis of Warren and Brandeis. They conceived the right of privacy as an extension of intellectual property, particularly copyright, which gives the individual the authority to decide whether and how to communicate “thoughts, sentiments, and emotions.” Warren & Brandeis, *supra*, at 198. The organizing principle of such protections is that “the individual is entitled to decide whether that which is his shall be given to the public.” *Id.* at 199. The right to prevent publication is thus “merely an instance of the more general right of the individual to be let alone,” *id.* at 205, in observance of the principle of an “inviolable personality,” *id.* From Warren and Brandeis, it was a small step to recognition of rights of personality that prohibit, *inter alia*, the commercial exploitation of a person’s likeness. *See, e.g., Trannel v. Prairie Ridge Media, Inc.*, 987 N.E.2d 923 ¶¶ 14-15 (Ill. Ct. App. 2013) (summarizing history of right of publicity among other privacy rights). BIPA is right at home in this setting. A requirement of written, fully informed consent before a person’s unique bodily identifiers are exploited by industry for competitive purposes is a straightforward instance of granting agency to the individual “to decide whether that which is his,” Warren & Brandeis, *supra*, at 199, shall be given

to private industry for competitive purposes and private gain. *See id.* at 213 (“[T]he law has no new principle to formulate when it extends this protection to the personal appearance . . .”).

Google’s argument that the Restatement formulation requires a “highly offensive” intrusion fails for two reasons. First, the argument overstates the importance of the Restatement’s characterization. Plaintiffs are not asserting a common-law privacy right for which the Restatement might actually supply the applicable test. If the Restatement is relevant, it is only as an indication whether rights under BIPA are part of the same historical legal landscape as other privacy rights for which standing is established — and indeed they are, not only as to the individual’s right to be free from offensive intrusion upon seclusion, *see* Restatement, *supra*, § 652B, but also as to “the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others,” *id.* § 652C, a right that “is in the nature of a property right,” *id.*

Second, even if it mattered whether Google’s unlawful behavior was highly offensive within the meaning of the Restatement, that question would clearly be for a jury to decide at trial, not for the Court to decide at summary judgment. If anything, summary judgment would be warranted in Plaintiff’s favor, not Google’s. The State of Illinois has already expressed on behalf of its citizens that collecting, storing and using such sensitive information without fully informed consent is sufficiently offensive to be prohibited by law. And common sense would tell any normal person that it is obnoxious to create, collect, store and commercially exploit face maps of other people without permission. Google’s argument that faces are public simply underscores how out-of-touch companies like Google have become. In Google’s world, it would indeed be perfectly fine for restaurants to dust their customers’ glasses for fingerprints and stockpile those identifiers. Surely a jury may reasonably disagree and find instead that Big Brother’s arrival is most unwelcome.

Through BIPA, the Illinois Legislature sought to defend a classic right of privacy closely related to other rights of privacy long recognized under American law. The harms BIPA recognizes are concrete, and its conferral of standing on Plaintiffs is unassailable.

2. Applicable Precedent Supports Plaintiffs' Standing

Google's photo-sharing competitor, Facebook, is facing a similar lawsuit in the U.S. District Court of the Northern District of California. *Patel v. Facebook, Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018). That case is further along than this one, and District Judge James Donato has all but done this Court's work for it. Before filing its motion for summary judgment, which that court denied, Facebook moved to dismiss the case against it for lack of standing on the same ground asserted here: concreteness. In a thorough and well-reasoned opinion, Judge Donato rejected that argument and held the injury inflicted by a BIPA violation to be concrete for purposes of standing.

These provisions, along with the plain text of BIPA as a whole, leave little doubt that the Illinois legislature codified a right of privacy in personal biometric information. There is equally little doubt about the legislature's judgment that a violation of BIPA's procedures would cause actual and concrete harm. BIPA vested in Illinois residents the right to control their biometric information by requiring notice before collection and giving residents the power to say no by withholding consent. As the Illinois legislature found, these procedural protections are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused. When an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.

Consequently, the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt. A violation of the BIPA notice and consent procedures infringes the very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is quintessentially an intangible harm that constitutes a concrete injury in fact. *See Spokeo II*, 867 F.3d at 1113 (and cases cited therein).

The Illinois legislature's considered judgments in enacting BIPA are also well-grounded in a long tradition of claims actionable in privacy law. The “common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person.”

Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017) (quoting *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763, 109 S.Ct. 1468, 103 L.Ed.2d 774 (1989)).

Id. at 953-54.

Google attempts to distinguish *Facebook* as decided in the context of a motion to dismiss, but that procedural distinction is without consequence. When Facebook again raised similar arguments in its later motion for summary judgment, the court endorsed its prior ruling “expressly reject[ing]” the “faulty proposition that plaintiffs must show an ‘actual’ injury beyond the invasion of the privacy rights afforded by BIPA.” *In re Facebook Biometric Info. Privacy Litig.*, No. 3:15-cv-03747-JD, 2018 WL 2197546, *1 (N.D. Cal. May 14, 2018).

Facebook, like Google, argued that actual harm was required, but the court rejected the argument, holding such harm unnecessary to a concrete injury to the right of privacy recognized in BIPA. *Patel*, 290 F. Supp. 3d at 954. Facebook, like Google, attempted to show consent through a user agreement and other evidence, but the court held those issues more suitable for resolution at summary judgment or trial. *Id.* at 956. Google does not even attempt to establish beyond genuine dispute that Plaintiffs gave the fully informed written consent required under BIPA. To the contrary, Google lacked permission from Plaintiffs to capture, store, and use face scans of them. (SAF 2.)

Google relies heavily on *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909 (7th Cir. 2017), in which failure to timely delete former customers’ information was held insufficient for standing. Similar facts were at issue in *Braitberg v. Charter Communications, Inc.*, 836 F.3d 925 (8th Cir. 2016) (retention of former customers’ information), and *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511 (D.C. Cir. 2016) (recording zip code). The plaintiffs in all of these cases directly provided the information in question to the defendants and complained only about how it subsequently had been handled. Similarly, the plaintiff in *Groshek v. Time Warner Cable, Inc.*, 865 F.3d 884 (7th Cir. 2017), allowed defendant to acquire a preexisting credit report. The present case involves an entirely different situation. Plaintiff Rivera gave Google nothing; a third party’s Droid phone instantaneously,

automatically, and inconspicuously uploaded photos of Rivera to Google Photos, where Google scanned and mapped her face, creating, collecting, storing and exploiting her biometric identifiers and information. Plaintiff Weiss gave Google photographs, not biometric identifiers or information, and that is a stark difference, as BIPA itself recognizes by excluding photographs from the definition of biometric identifiers. 740 Ill. Comp. Stat. Ann. § 14/10. Plaintiffs' biometric identifiers and information did not exist until Google created, collected, stored and used them for its own competitive purposes to enhance its photo-sharing services. Without the fully informed, written consent required by BIPA, Plaintiffs had no reason to think their actions would result in Google's creating, collecting, storing, and exploiting their sensitive bodily identifiers and information.

Google also relies on *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017), *aff'd in part, vacated in part sub nom. Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017). The plaintiff in that case, however, had performed a lengthy face-scanning operation and uploaded it to the defendant's server so that the plaintiff's face could be used during online gameplay. *Id.* at 14 ("The 3-D mapping process uses cameras to capture a scan of the gamer's facial geometry, which is then used to disseminate a realistic rendition of the gamer's face. Gamers must hold their faces within 6 to 12 inches of the camera and slowly turn their heads 30 degrees to the left and to the right during the scanning process. The process of scanning the face takes about 15 minutes." (citations omitted)). And before undertaking that complicated and unmistakable face-mapping process, the plaintiff had agreed to a disclosure stating "[y]our face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay," *id.*, and referring to the terms of a user agreement, *id.* The court ruled:

No reasonable person, however, would believe that the MyPlayer feature was conducting anything other than such a scan [of face geometry]. Plaintiffs had to place their faces within 6 to 12 inches of the camera, slowly turn their heads to the left and to the right, and do so for approximately 15 minutes. This degree of invasiveness far exceeded that of a simple photo, and plaintiffs do not plausibly assert (beyond a mere conclusory allegation) that they would have withheld their consent had Take-Two included the missing term.

Id. at 15-16.

The decision in *McCullough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016), rests on the same judicial realpolitik as *Take-Two*. The plaintiff rented a storage locker for which access was controlled by a fingerprint scanner, and the rental process required submission to an initial fingerprint scan. *Id.* at *1. In holding for the defendant, the court explained that “McCullough undoubtedly understood when she first used the system that her fingerprint data would have to be retained until she retrieved her belongings from the locker.” *Id.* at *3.

The facts of the present case are entirely different from *Take-Two* and *McCullough*.³ Plaintiffs did not participate in a fifteen-minute face-scanning procedure for the express purpose of creating a 3-D face map to be uploaded to Google’s servers, and they did not submit to fingerprinting. Plaintiff Rivera is not even a user of Google photos and thus did not upload photos to Google. (Response to SUF 31.) Plaintiff Weiss is a user but simply took pictures that were instantaneously, automatically and inconspicuously uploaded and scanned without any affirmative acts by Weiss. (Response to SUF 24, 30.) Contrary to Google’s disingenuous characterization of Plaintiff Weiss’s deposition testimony on the subject, he clearly testified that he would not have given consent if Google had asked him to do so. (See Response to SUF 29 (citing Maya Decl. Ex. A (Weiss Depo Excerpts) at 144:4-15, 145:4-9 (testifying he would have found a request for permission to collect his biometrics “disturbing”); *id.* at 171:21 (“I would not have consented if I had known that biometric information was being gathered, collected, stored.”); SAF 2.)

Google argues that Plaintiffs gave post-hoc consent to the violations. In Rivera’s case, Google argues she continued to allow photographs to be taken of herself despite the possibility that a third

³ In a recent opinion, Judge Gottschall distinguished *Take-Two* and *McCullough* and found Article III standing. See *Monroy v. Shutterfly*, No. 16 C 10984, 2017 WL 4099846, at fn. 5 (N.D. Ill. Dec. 21, 2017) (finding Article III standing exists where plaintiff alleged the defendant collected his face scans without his knowledge in violation of BIPA).

party might use a Droid device that would upload the images to Google Photos. In Weiss's case, Google argues he continued using Google photos after learning what Google was doing. But neither shunning photography nor shunning Google Photos would have made any practical difference at that point because Plaintiffs' faces already had been scanned and mapped many times over. Moreover, Mr. Weiss encountered difficulty attempting to disable Google Photos (Response to SUF 10) and, in any event, Google's arguments are at most an attack on witness credibility for a jury to weigh at trial, not for the Court to weigh on summary judgment.

3. The Violation Plainly Caused the Injury

Plaintiffs' injuries under BIPA occurred when Google created, collected, stored, and used their photos for its own competitive purposes. Nothing Plaintiffs subsequently did changes that fact.

As noted above, Google contends that Plaintiffs would not have acted differently even if Google had bothered to obey the law — a proposition flatly contradicted by Plaintiffs' consistent and clear deposition testimony on the subject, which Google ignores. (*See* SAF 2.)

Fundamentally, however, Plaintiff Rivera did not "act" in any way in relation to Google. She is not and has never been a Google Photos user. (*See* Response to SUF 31.) Her image was uploaded and processed instantaneously, automatically, and inconspicuously when a third party took her picture. Google faults her for continuing to allow herself to be photographed by third parties after learning of Google's illegal activity, though Ms. Rivera testified that she did not know Ms. Gutierrez was uploading any such photos to Google Photos at the time. (*See* Response to SUF 37.) Even assuming that Ms. Rivera had some duty to withdraw from photography (a rather unreasonable proposition), her face had already been scanned and mapped many times at that point. Google fails to explain how shunning photography would have changed anything.

Plaintiff Weiss testified that he learned that Google Photos (which came pre-installed on his phones) was collecting his facial biometrics from photographs in late 2015, while he lived in Illinois. (*See* Response to SUF 30). Mr. Weiss encountered difficulty turning off the "face grouping" feature

in Google Photos until December 2017, but even if he had done so earlier, no evidence suggests that

[REDACTED]. (See Response to SUF 10.) Rather, whenever a photograph is uploaded through Google Photos to Google, Google has [REDACTED]

[REDACTED],” and then Google [REDACTED]

[REDACTED].

(Maya Decl. Ex. D (Ko Depo Excerpts) at 39:20-23; *see also* Maya Decl. Ex. G (Plaintiffs’ Depo Ex. 9); Response to SUF 10.) As with Ms. Rivera, Mr. Weiss’s face had already been scanned and mapped many times before he learned what Google was doing, and there was nothing either Plaintiff could do to stop the process or retroactively stop Google’s unauthorized collection of their facial biometric data.

Because the injuries occurred when Google created, collected, stored, and exploited Plaintiffs’ biometric identifiers and information, none of which existed until Google’s unlawful actions, Google’s unlawful conduct directly caused Plaintiffs’ injuries.

B. Plaintiffs Are Aggrieved Within the Meaning of BIPA

BIPA provides a private right of action to “[a]ny person aggrieved by a violation of this Act.” 740 Ill. Comp. Stat. Ann. § 14/20. Google argues that even if it violated BIPA, Plaintiffs do not qualify as persons aggrieved by the violations.

1. Plaintiffs Are Aggrieved As a Matter of Statutory Interpretation

As explained above, the right of privacy recognized in BIPA is squarely within the historical path of American privacy law. A new chapter has been written in response to a wave of new technology, but it is still the same story. The invasion of Plaintiffs’ privacy rights is therefore no different than the invasion of countless other privacy and other interests that are not necessarily pecuniary but no less actionable. (*See supra* Part IV.A.1.)

The rights recognized under BIPA empower individuals to decide whether to engage at all in the realm of biometric identification. When a company like Google strips the individual’s agency “to

decide whether that which is his” will be taken, held, and used by another, the essence of the right is violated. Warren & Brandeis, *supra*, at 199. No more is needed for the individual to be aggrieved.

Notably, Facebook made the same argument as Google about the meaning of the term “aggrieved,” and the Northern District of California rejected the argument in the course of its thorough and well-reasoned decision granting class certification. Quoting its prior ruling in *Patel*, the court held:

[A] plain of reading of BIPA “leave[s] little question that the Illinois legislature codified a right of privacy in personal biometric information” rooted in “a long tradition of claims actionable in privacy law” and extending to control over one’s data, independent of disclosure or misuse risks. *Patel*, 2018 WL 1050154, at *4. This intent cannot be squared with a construction of “aggrieved” that requires some other “actual” injury, whatever that might be, particularly when deprivation of BIPA’s notice and consent requirements amounts to the “precise harm the Illinois legislature sought to prevent.” *Id.*

In re Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD, 2018 WL 1794295, at *7 (N.D. Cal. Apr. 16, 2018). Moreover, the court observed, other Illinois statutes clearly limit private rights of action to those who suffer actual injury, while BIPA has no such limitation.

[T]he Illinois legislature clearly knows how to condition a cause of action on actual injury simply by saying so in the statute. *See, e.g.*, 815 Ill. Comp. Stat. Ann. 505/10a (Illinois Consumer Fraud and Deceptive Business Practices Act) (private right of action limited to person who suffers “actual” damage). The legislature did not choose to say so in BIPA, and that choice must be given weight.

Id.

BIPA recognizes individuals’ agency over their biometric identifiers. Stripping that agency violates that right. Google did just that, and Plaintiffs are aggrieved under the statute.

2. Plaintiffs Are Aggrieved As a Matter of Precedent

The Illinois Supreme Court has already interpreted the meaning of the term “aggrieved” in an Illinois statute. In *American Surety Co. v. Jones*, 51 N.E.2d 122 (Ill. 1943), the court reiterated its already longstanding definition of the term as including ““when a legal right is invaded by the act complained of,”” *id.* (quoting *Glos v. People*, 102 N.E. 763, 766 (Ill. 1913)), and as ““having a substantial grievance; a denial of some personal or property right,”” *id.* (quoting *Glos*, 102 N.E. at 766).

In other words, aggrieved parties are those with a “direct, immediate and substantial interest rather than a speculative, theoretical, inconsequential or remote interest.” *Id.* at 126. The plaintiffs in *American Surety* were insurance companies challenging the Illinois insurance regulator’s renewal of authorization for Lloyds of London to transact business in the state. The court rejected plaintiffs’ challenge because “none of their certificates were involved” and “[a]ny prejudice resulting to them . . . was at most an indirect or inconsequential result thereof.” *Id.* at 125.

In the present case, Plaintiffs clearly are aggrieved under the meaning the Illinois Supreme Court has given that term. They do not challenge actions directly affecting third parties in hopes of indirectly benefiting themselves. They challenge unlawful conduct that directly invaded their own rights. Google illegally created, collected, stored, and exploited Plaintiffs’ own biometric identifiers and information. The right to permit or refuse such activity belongs to Plaintiffs, and Google’s invasion of the right leaves Plaintiffs aggrieved under Illinois law.

Google places essentially all its chips on the intermediate appellate court decision in *Rosenbach v. Six Flags Entertainment Corp.*, 2017 Ill. App. 2d 170317 (Ill. App. Ct. 2017). That is a bad bet. This Court “must make a predictive judgment as to how the supreme court of the state would decide the matter if it were presented presently to that tribunal” and, for a number of reasons, *Rosenbach* is of no value in weighing how the Supreme Court of Illinois would decide this case, and thus of no value to the present analysis. *Allstate Ins. Co. v. Menards Inc.*, 285 F.3d 630, 635 (7th Cir. 2002).

First and foremost, and as the *Facebook* court observed, *Rosenbach*’s failure to consider *American Surety* is both telling and troubling, all the more so because *Rosenbach* cited case law from Wisconsin instead. See *Facebook*, 2018 WL 1794295, at *7 (“Tellingly, *Rosenbach* omits any discussion of *Jones*, and Facebook also does not address it in its papers. That is a concern because *Jones* is good law in Illinois and is actively cited today by other federal courts and Illinois state courts, significantly in the BIPA context. A convincing construction of ‘aggrieved’ in BIPA would need to account for *Jones*, and not rely entirely, for example, on decisions from courts outside Illinois.”)

(citation omitted). *Rosenbach* fails to even acknowledge *American Surety* — the controlling Illinois Supreme Court authority on the meaning of the term “aggrieved” under Illinois law. Whether that failure was intentional or negligent, it leaves *Rosenbach* in tension if not outright conflict with higher, controlling authority.

Second, *Rosenbach* expressly limits its own reach to the facts of the case. And those facts are essentially the same as in *McCullough*: a plaintiff who submitted to fingerprinting in connection with a season pass to an amusement park later complained that the required notices were deficient. *Rosenbach*, 2017 Ill. App. 2d 170317 ¶ 7. The court held this “mere technical violation of the Act” insufficient, *id.* ¶ 18, but with two major caveats: (1) that the plaintiff “did not allege in her complaint any harm or injury to a privacy right,” *id.* ¶ 20 n.1; and (2) that “the injury or adverse effect need not be pecuniary,” *id.* Here, by contrast, Plaintiffs have alleged and clearly established a violation of their privacy rights under BIPA, and they have maintained from inception that their injuries lie in the invasion of those rights rather than in pecuniary loss. *Cf. Facebook*, 2018 WL 1794295, at *8 (stating that “the facts in *Rosenbach* place it several steps away from this case” because “an express request for a fingerprint scan is a far cry from the situation here”).

Because *Rosenbach* is inapposite, Google’s citation of inferior state courts slavishly following *Rosenbach* adds nothing. Similarly, Google relies again on *Gubala*, *Sterk*, and *Padilla*, but as explained previously, those cases involved the dissimilar circumstance of companies that properly acquired data but retained it for too long. By contrast, Google from inception illegally created, collected, stored, and exploited the data for its own competitive purposes in the market for photo-sharing services, which Google is uniquely well-positioned to exploit in order to serve its users “ [REDACTED] ” (SAF 6.)

The deprivation of the central right recognized in BIPA — Plaintiffs’ right to decide whether to allow their own biometric identifiers and information to be created, collected, stored, and exploited — is all the harm that is required for Plaintiffs to be aggrieved within the meaning of BIPA.

The Motion should be denied.

C. Plaintiffs Are Entitled to Statutory Damages and Injunctive Relief

Section 20 of BIPA provides for statutory damages and injunctive relief.

A prevailing party may recover for each violation:

- (1) against a private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or actual damages, whichever is greater;
- (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is greater;
- (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
- (4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 Ill. Comp. Stat. Ann. § 14/20.

Google argues that even if it has committed the violations alleged by Plaintiffs, neither statutory damages nor injunctive relief can be awarded. The Court should reject Google's attempt to shirk responsibility.

1. Statutory Damages

BIPA provides "liquidated damages of [\$1,000/\$5,000] or actual damages, whichever is greater." *Id.* Google argues that liquidated damages provisions in private contracts must be reasonable approximations of actual damages or they will not be enforced, and that federal courts have extended the idea to statutory damages provisions. (Mot. at 27-28.) The extension to the statutory context, however, is vastly overstated.

First, the decisions cited in the Motion rest primarily on statutory interpretation, and each of the statutes in question was held to require at least some actual damages before liquidated damages could be awarded. The statute at issue in *Doe v. Chao*, 540 U.S. 614 (2004), provided for recovery of "actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a

person entitled to recovery receive less than the sum of \$1,000,” *id.* at 619. The question before the Court was “whether plaintiffs must prove some actual damages to qualify for a minimum statutory award of \$1,000,” and the Court held that “they must.” *Id.* at 616. The primary reason for the Court’s conclusion was the plain statutory language, which provides for actual damages sustained and then guarantees a minimum amount to those already “entitled to recovery” — *i.e.*, those who already can show actual damages. *Id.* at 620 (holding that the “simplest reading” of the clause “a person entitled to recovery, . . . looks back to the immediately preceding provision for recovering actual damages”). Similarly, the statute before the Seventh Circuit in *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535 (7th Cir. 2012), provided for “actual damages but not less than liquidated damages in an amount of \$2,500,” *id.* at 537 (quoting 18 U.S.C. § 2710(c)(2)(A)). The court in *Sterk* regarded the statutory language at issue in *Doe v. Chao* as “even less indicative that an actual injury must be proved to entitle the plaintiff to statutory damages.” *Id.* at 538. The court in *Van Alstyne v. Electronic Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009), followed *Doe v. Chao* because the statutes at issue in the two cases were materially indistinguishable, *Van Alstyne*, 560 F.3d at 205. And the court in *Padilla v. DISH Network L.L.C.*, No. 12-cv-7350, 2014 WL 539746, at *2 (N.D. Ill. Feb. 11, 2014), followed *Doe* and *Sterk* because the statute before the court was “nearly identical” to the one in *Sterk*.

A different result is warranted here because the statutory language is different. BIPA provides for liquidated damages as an alternative to actual damages, not as a minimum amount of actual damages. The statute uses the disjunctive “or”: “liquidated damages of [\$1,000/\$5,000] or actual damages, whichever is greater.” 740 Ill. Comp. Stat. Ann. § 14/20. Unlike *Sterk*, where the court observed that “zero” actual damages was inconsistent with the statutory language, an actual damages amount of “zero” is perfectly sensible under BIPA for the simple reason that \$1,000 or \$5,000 is “greater” than zero. The court in *Facebook* rejected the same argument for the same reasons. *In re Facebook Biometric Information Privacy Litig.*, No. 3:15-cv-03747-JD, 2018 WL 2197546, at *6 (N.D. Cal. May 14, 2018) (“[Facebook’s argument] also misconstrues the plain language of BIPA.

Section 20 expressly provides for two separate categories of damages that a plaintiff may recover. Consequently, proof of actual damages is not a prerequisite to recovery of statutory damages.”); *see also id.* (distinguishing *Doe v. Chao* because “[t]he statutory damages provision at issue in *Doe* is far too different from the language in BIPA to serve as a sound basis for analogy or guidance here.”).

Second, as discussed above, Plaintiffs have indeed suffered actual harm, even if that injury is not easily translated into monetary damages. Again, this is nothing unusual in the realm of law and remedies, where intangible losses are translated into dollars and cents every day. *Sterk* confirmed the compensable injuries inflicted here when it distinguished *Pichler v. UNITE*, 542 F.3d 380 (3d Cir. 2008), and *Kehoe v. Fidelity Federal Bank & Trust*, 421 F.3d 1209 (11th Cir. 2005), on the basis that “[i]n both *Pichler* and *Kehoe* there was an unlawful appropriation of private personal information, and as the courts pointed out this is a perceived although not a quantifiable injury.” *Sterk*, 672 F.3d at 539. In the present case, there can hardly be a dispute that Google unlawfully appropriated Plaintiffs’ biometrics in violation of BIPA. The automated creation, collection, and storage of biometric identifiers without fully informed written consent is plainly unlawful in the State of Illinois. Google may regard individual states’ pesky laws as inconvenient to its worldwide master plan, but its actions are unlawful nonetheless. The automated creation, collection, and storage of biometric identifiers and of biometric information that should not exist, and that would not exist but for Google’s unlawful conduct, inflicts cognizable legal injury compensable in either actual or liquidated damages. If Plaintiffs choose to seek liquidated damages, that is because they are free to elect their preferred remedy under the terms of the statute, not because they have suffered no harm.

2. Injunctive Relief

The Motion makes a half-hearted pass at arguing injunctive relief is unavailable, simply stating that Plaintiffs cannot establish the elements of injunctive relief, “especially” irreparable harm. (Mot. at 29.) Such a throwaway presentation does not begin to carry a defendant’s burden on a motion for

summary judgment and cannot be taken seriously. Moreover, injunctive relief plainly would be warranted if Plaintiffs prevailed.

Whether to award injunctive relief “generally requires a court to consider (1) whether the plaintiff has suffered or will suffer irreparable injury, (2) whether there are inadequate remedies available at law to compensate for the injury, (3) the balance of hardships, and (4) the public interest.” *Sierra Club v. Franklin County Power of Ill., LLC*, 546 F.3d 918, 935 (7th Cir. 2008). A complete four-part analysis is not even necessary “when a plaintiff prevail[s] on the merits of his claim, or when, in an action for a statutory injunction, a violation was demonstrated and there [i]s a reasonable likelihood of future violations.” *Id.* (citation omitted). Nor is it necessary to balance equities “where the defendant’s conduct has been willful.” *Id.*

Here, Plaintiffs will suffer irreparable injury unless and until injunctive relief is awarded. The Court has the power to order Google to destroy the biometric identifiers and information that should never have existed and that would not have existed but for Google’s unlawful conduct. All of the four factors favor injunctive relief. It is Plaintiffs’ right, not Google’s, to decide whether to allow the creation, collection, storage, and exploitation of their biometric identifiers and information, and for Google to arrogate that decision to itself works irreparable harm. Plaintiffs cannot be made whole by any remedy at law because they do not wish to place their rights of privacy and personal autonomy up for sale. The hardship is entirely on Plaintiffs, as Google could easily stop its unlawful conduct within the State of Illinois, for example by turning off the offending features for devices with Illinois IP addresses. And the public interest overwhelmingly favors injunctive relief. Abuses of consumers’ privacy by technology giants have recently made headlines and summoned industry titans to testify before Congress. Yet Google continues to openly flout the policy judgment of the State of Illinois that fully informed written consent is required before a citizen surrenders biometric identifiers and information. If the rule of law is to be respected, then the law must override Google’s pursuit of its own market objectives.

Moreover, the four factors will likely fade in relevance as this case proceeds. The four-part analysis will not even be necessary if Plaintiffs prevail on the merits (they will), if a statutory violation is demonstrated and found likely to continue (it is continuing), or if the defendant's conduct is willful (which it is).

V. CONCLUSION

For the foregoing reasons, the Motion should be denied.

Dated: May 21, 2018

Respectfully submitted,

By: /s/ Katrina Carroll
Katrina Carroll
kcarroll@litedepalma.com
Kyle A. Shamberg
kshamberg@litedepalma.com
Lite DePalma Greenberg, LLC
211 West Wacker Drive, Suite 500
Chicago, Illinois 60606
Telephone: (312) 750-1265

AHDOOT & WOLFSON, PC
Robert Ahdoot (pro hac vice)
radhoot@ahdootwolfson.com
Tina Wolfson (pro hac vice)
twolfson@ahdootwolfson.com
Theodore Maya (pro hac vice)
tmaya@ahdootwolfson.com
Bradley K. King (pro hac vice)
bking@ahdootwolfson.com
10728 Lindbrook Drive
Los Angeles, California 90024
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

**CAREY RODRIGUEZ
MILIAN GONYA, LLP**
David P. Milian (pro hac vice)
dmilian@careyrodriquez.com
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Telephone: (305) 372-7474

Facsimile: (305) 372-7475

Counsel for Plaintiff and the Putative Class